Cloud Computing
The INL Experience

Linda Guinn Montgomery
General Counsel, Battelle Energy Alliance, LLC

April 26, 2012

www.inl.gov

Idaho National Laboratory

Type	Consumer Activities	Provider Activities
SaaS (Software as a service)	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS (Platform as a service)	Develops, tests, deploys, and manages applications hosted in a cloud environment.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS (Infrastructure as a service)	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

A Government Cloud

- Reforming federal government, including cloud computing, included in President's inagural address
- *25 point implementation plan to reform government IT*, Office of Management & Budget (OMB) Chief Information Officer, December 9, 2010
  - Shift to "Cloud First" policy.
  - Each agency will identify three "must move" services within three months, and move one of those services to the cloud within 12 month and the remaining two within 18 months
- *Federal Cloud Computing Strategy*, OMB Chief Information Officer, Feb. 8, 2011. Online: www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pd
- New government apps store: https://www.apps.gov/cloud/main/start_page.do
- Standards: http://www.nist.gov/itl/cloud/index.cfm
- Chief Information Office dashboard: http://www.cio.gov/techstat/
- GSA standard agreement: https://forum.webcontent.gov/resource/resmgr/model_amendment_to_tos_for_g.pdf

Idaho National Laboratory

Why a "Cloud First" Policy?

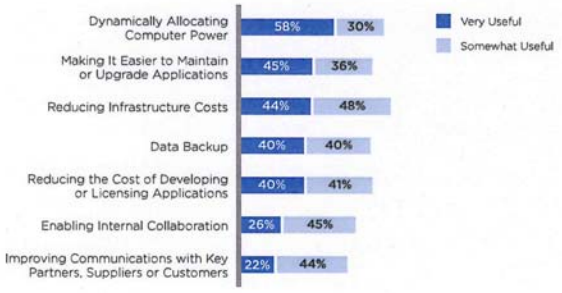
- Cloud computing brings a wide range of benefits
  - *Economical*: Cloud computing is a pay-as-you-go approach to IT, in which a low initial investment is required to begin, and additional investment is needed only as system use increases.
  - *Flexible*: IT departments that anticipate fluctuations in user demand no longer need to scramble for additional hardware and software. With cloud computing, they can add or subtract capacity quickly and easily.
  - *Fast*: Cloud computing eliminates long procurement and certification processes, while providing a near-limitless selection of services.

Chief Information Officer in *The Federal Cloud Computing Strategy*

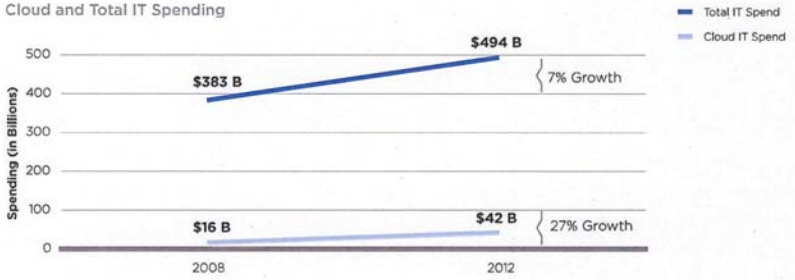
The promise of improved agility and lower costs is leading organizations to consider broad adoption of cloud computing.

GROWING ACCEPTANCE OF CLOUD COMPUTING

IT Objectives Furthered by Cloud Capabilities
Percentage of Respondents



Cloud and Total IT Spending



[1] Vaquero, Luis M, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, Volume 39 Number 1 (January 2009): 52.

From the AUDIT DIRECTOR ROUNDTABLE* of the CORPORATE INTEGRITY PRACTICE
www.adrexecutiveboard.com

Infrastructure-as-a-service has the highest level of risk associated with it.

- Laws and regulations in some countries can limit the use of cloud computing, especially if personal, financial, or tax records are transferred and stored overseas.

RISKS ASSOCIATED WITH CLOUD DELIVERY MODELS

Risks	SaaS	PaaS	IaaS
Effect of malicious co-tenants	◕	◕	◕
Isolation failure	◕	◕	◕
Incomplete or ineffective deletion of data	◕	◕	◕
Conflicting provider security procedures	◐	◐	◐
Unclear location of data	◕	◕	◕
Service portability	◐	◕	◕
Resource limitations	◔	◐	◕
Remote access vulnerabilities	◕	◕	◕
Service hacking	◕	◕	◕
Lack of compliance assurance	◐	◐	◕
Lack of transparency in supply chain	◐	◐	◐
IP protection	◔	◐	◕
Loss of governance	◕	◕	◕
Abuse of privilege at provider's end	◕	◕	◕
Business continuity planning and disaster recovery security	◔	◐	◕

◔ Low Risk
◐ Medium Risk
◕ High Risk

Source: ENISA, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport, November 2009.

From the AUDIT DIRECTOR ROUNDTABLE* of the CORPORATE INTEGRITY PRACTICE
www.adrexecutiveboard.com

Why INL Chose the Cloud

- Decision point for email:
  - Upgrade Lotus Notes or
  - Transition to a new system
- Lotus not very friendly to other systems
- Aggressive time table forced us to become an early adopter.
- E-discovery currently done "by hand", machine by machine – no search capability

Idaho National Laboratory

RFP Requirements

- Small business provider
- System had to meet federal security standards (Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347) and then update to the new FedRamp – Federal Risk and Access Management Program)
- Servers must be located in the U.S.
- Information must be encrypted *in flight* and *at rest.*
- Must have method for clean-up, if classified information spillage occurred.
- Unclassified subcontract (no FOCI)
- Database/search capacity for e-discovery

Issues

- Classified Information
  - Fear
  - Slippage clean-up (by whom)
- Encryption
- Indemnification
- Export Control
  - State (ITAR) v. Commerce (EAR) positions
  - DOE and NRC
  - Use of collaboration tools
- Appropriate retention times?

Idaho National Laboratory

Indemnification

- Separate “user agreement” required by Google.
- Indemnification by BEA
  - BEA provided bridge to start implementation
- Contracting Officer letter authorizing indemnification
  - Field Office delegation
  - Antideficiency Act compliance

Export Control Issue

- GSA solution:
  - Limited to no export controlled information
  - Limited system support to approved people.
- Google barred ITAR information from the system.
  - U.S. servers, but administrators world-wide
  - INL would encrypt (per procedures) before entering system.
  - Google would accept assurances from State

Idaho National Laboratory

Were is the INL now?

- DOE issued export control/indemnification letter for INL only.
- DOE working an interagency export control policy.
- We are struggling with correct encryption (Entrust is “clunky”).
- INL further ramping up company training.
- Found that our solution didn’t work well for mobile devices (working).
- Doing phased implementation, but behind schedule.
- Expect this solution will solve our e-discovery issues.

Lessons Learned

- Even "off the shelf" will require work-arounds.
- Educate/Communicate.
  - Fear translates into "No" or great reluctance.
  - Lunch & Learn outreach is working.
  - Early education of key advocates (senior staff's admins).
- Be crystal clear who owns the information and whether any ancillary uses are allowed.
- Integrated implementation teams are a must.
- Worthwhile to do contemporaneous due diligence.

Idaho National Laboratory

Lessons Learned - Security

- Issues related to classified information on an unclassified system.
  - FOCI
  - Security Clearances
  - Policy of "removing" v. "removing access"
- Identification of foreign nationals
  - Previously physically excluded from system
  - Now have to identify and structure access

Lessons Learned – Export Control

- Highlights inadequacies in current systems
- No new risk exposure – but greater sensitivity and scrutiny
- Have to cover all major regulators:
  - Commerce Dept.
  - State Dept.
  - DOE
  - NRC
- Great learning opportunities for employees

Idaho National Laboratory

Lessons Learned - Escrow

- Escrow Agreement for another provider as "back-up".
  - Disaster recovery
  - Facilitate transfer if unhappy with contractor
  - Limit interruption of service
  - Holds the data, but not underlying system
  - Verify data
    - 76% of deposits into escrow were incomplete;
    - 81% of deposits into escrow could not be used without additional help from the developer

- www.ironmountain.com/escrow
- www.ironmountain.com/escrowfordummies

Summary

- Cloud computing is here to stay.
- Cloud computing has significant advantages.
- Government cloud computing standards are drafted but not final.
- Risks have to be recognized to be able to be addressed.
- Risk mitigation strategies are developing and available information is increasing.
- http://www.cio.gov/cloudbestpractices.pdf